ON THE SECURITY RISKS OF THE BLOCKCHAIN

ABSTRACT

The adoption of blockchain technology is taking place at a fast pace. Security features inherent in blockchain make it resistant to attack, but they do not make it immune, and blockchain security risks do exists. This paper details the associated risks and concerns of the blockchain. We explore relevant standards and regulations related to blockchain and survey and analyse 38 blockchain incidents to determine the root cause in order to provide a view of the most frequent vulnerabilities exploited. The paper reviews six of these 38 incidents in greater detail. The selection is made by choosing incidents with the most frequent root cause. In the review of the incidents, the paper details what happened and why and aims to address what could have been done to mitigate the attack. The paper concludes with a recommendation on a framework to reduce cyber security risks when using blockchain technologies.

Keywords: security; standards; blockchain; root cause analysis; security recommendations

INTRODUCTION

The Blockchain technology was devised by Satoshi Nakamoto, the designer of Bitcoin, set out in a white paper in 2008[1]. The technology created a 'peer-to-peer' online cash system, whereby a third party, such as a financial institution, was no longer needed. The benefits of using such a technology are transparency, authenticity and auditing as it takes away the need for trust between two parties participating in a transaction[2].

Since the inception of the Blockchain, several hacks and attacks have occurred, bringing into question the security of the technology. The causes of these incidents range from smart contract vulnerabilities[3], application vulnerabilities[4], cloud infrastructure/server breach[5], insider breaches to social engineering breaches[6]. Some of the causes are not publicly known. A study performed by Luu et al.[7] discovered that 8,833 out of the 19,366 existing Ethereum contracts are vulnerable. Atzei et al.[8] analysed the security vulnerabilities of Ethereum smart contracts, and provided a taxonomy of common programming pitfalls that may lead to vulnerabilities, Zimba et al.[9] investigated crypto mining attacks by examining malware code and suggested mitigations, while Li et al.[10] analysed the vulnerabilities in Blockchain systems and compiled a list of security risks to Blockchain systems.

Yet current research places an imbalanced focus on the technical aspects of Blockchain. There is limited work in regulatory frameworks, Blockchain standards and best practices. Presently, businesses and organisations operate under a lack of standards, where there is currently only one in development[11]. This creates legal liability issues as Blockchain systems often run on cloud platforms and integrate with 3rd party applications, notably in a public and consortium driven type[12], and to date it is unclear how legal liabilities are determined if Blockchain incidents do occur. Therefore, there is a need to understand and identify the applicability of the existing standards and regulations that are connected to Blockchain.

Ideally, organisations learn lessons from previous incidents. Public information sharing is necessary at the earliest opportunity. This also allows new industries adopting the technology to learn from other communities, as despite their reasons for using the Blockchain may be different the vulnerabilities remain the same. Although some incidents are publicly known, the information is not always complete or accurate. As a result, organisations cannot effectively benefit from the mistakes of others, since there doesn't seem to exist a procedure to properly document and report incidents. However, experience can be borrowed from the general cyber security area related to the incident response (IR). A complete IR lifecycle encompasses incident identification, notification, analysis, containment, mitigation, incident learning and dissemination, where lessons learned are cycled back to the incident identification stage of the IR lifecycle[13].

In this paper we identify current security and other standards that may be pertinent for the blockchain technology. Through the examination of existing cases of security breaches based on a root cause analysis approach, we analyse Blockchain security incidents with a focus on standards, information governance and regulatory frameworks. This analysis informs a set of recommendation on what a cyber security blockchain framework should include and have implications for the creation of the Blockchain specific security standard.

AN OVERVIEW OF THE BLOCKCHAIN TECHNOLOGY

'Blockchain' or 'Blockchain technology' is seen as the backbone of the Bitcoin protocol, and as an online, distributed and publicly available ledger that is updated by the nodes of a peer-to-peer (P2P) network, based on consensus, without the mediation of a trusted third party, where all transactions are secured by cryptographic means[14]. The blockchain is essentially a very restricted data structure, which is open, public and append only.

It contains all transactions ever made within 'blocks', each of which contains groups of transactions, linked together based on cryptography rules[15]. Regardless of whether the transactions are purely financial or not, the underlying mode of operation is always the same (Figure 1). First a transaction request is made and broadcasted across a network of peers. This could be a contract, an update of a record, a financial transaction or anything that is transactional information. The nodes check the validity of the transaction through a process called mining, trying to solve a very difficult computationally-wise mathematical problem, which is resource-intensive, and then broadcast the solution to the other miners for confirmation. Once confirmed, the original miner is rewarded in bitcoins for their effort and the transaction itself is then added into a confirmed block. This block is timestamped and linked to the previous block, because the very solution to the mathematical problem is based on the unique cryptographic signature (hash) of the previous block. This means that all blocks are linked together in sequence, i.e., there is a clear and unique path from block 0 all the way to block n[16].

[Figure 1 about here]

As blocks are identified, miners add them in their local copy of the blockchain and broadcast them to the network. The rest of the miners, when they receive the information about this newly identified block, they validate it (which is not resource-intensive like mining), and assuming that the information is indeed validated, i.e., the solution to the mathematical problem is correct, then they also update their local copy of the blockchain. As a result, all miners across the network have access and maintain to the same copy at all times[15].

Blockchain Typology based on access rights

Blockchains can be categorised in different ways. Okada et al. propose their classification based on the existence or absence of a trusted authority with certain control over the chain, and the existence or absence of incentives in the form of an operational market around the blockchain system[17]. Equally, other classifications have to do with the permission rights and the ownership of the chain, or the degree of decentralisation and the computing approach for service delivery (peer to peer or cloud-based). One can identify three main types of blockchains: public, private and consortium-driven. Public blockchains are permissionless and anyone can send transactions as well as participate in the process of deciding whether a given block gets added to the overall chain. In addition, third parties and intermediaries are not needed, or needed to be trusted. Private and consortium blockchains are both types of permissioned chains. In a private blockchain, one organisation owns the 'write' permissions. 'Read' permissions can be made available to the public or trusted others if necessary via the authorisation of the owner organisation. As a result, private blockchains are permissioned and need somebody trusted for the chain to operate[18]. This is ideal for database management or auditing within a single company. In a consortium blockchain, the validation process is controlled by several pre-selected nodes[19]. For example, the rules of the blockchain may be that two banks and a regulator must sign each block for it to be added. Again, the right to read the blockchain can be made public if required and consortium-based blockchain can be thought of as partially decentralised[20].

RISKS AND CONCERNS IN THE BLOCKCHAIN ERA

Blockchain technology provides opportunities for businesses to improve efficiency and reduce costs, however, inherent risks must be considered and understood by firms. In this

section we present an aggregation of these risks based on the classification of permissionless and permissioned chain risks.

Permissionless blockchain

Currently, more than half of the network's processing (hashing) power rests in a single country's hands, namely China[21], thanks to cheap energy and loose regulatory frameworks about emissions[22]. This could lead to the possibility of collusion and threaten the democratic nature of a public blockchain[23]. The Chinese government has begun banning some conversions between virtual currencies, such as bitcoins[24], and cracking down on mining, in an attempt to reduce power shortages[25]. Such an outcome may very well push mining pools to move to alternative countries with less regulated environment and equally cheap electricity, shifting the balance and making another country the leader in mining and hashing power. However, the problem of one country being dominant over the network would still persist[26].

The strength of the Bitcoin protocol is that it is open source, and publicly available to everyone, meaning that everybody can examine the code. However, this is a double-edged sword: upon identifying a weakness in the code, one may alter the network, but equally, may be less benevolent and choose to exploit the unknown security vulnerabilities through a zero-day attack[27]. Another threat is that of time jacking attacks[28]. Time jacking is initiated when an attacker announces an inaccurate timestamp for a block. As the attacker is connected to other nodes, they may accept this inaccurately timestamped block, and as a result the network time counter speeds up for the majority of the miners. In essence, there will be a fork created for the blockchain, with miners adding new blocks in a longer chain which has been tampered with. The consequence is that there are opportunities for double-spending, i.e., the same cryptocurrencies spent more than once. In addition, it would lead to wasting valuable computational resources during mining, as benevolent miners will be mining for the counterfeit chain[15].

Next, a risk that pertains to cryptocurrencies has to do with their storage. In fact, the most popular mode of storage for crypto-currencies, i.e., online and mobile cryptowallets, are quite insecure. A cryptowallet is a collection of private keys and several users today store their private keys in internet based, and thus hack-prone, wallets[29]. The best practice is generally to avoid using such 'hot' wallets and instead use cold storage, such as USB Drives, offline wallets or even paper-based wallets documents. It is worth mentioning, however, that even these practices have security weaknesses[30]. For this reason, there are studies that attempt to provide more secure and more reliable approaches to cryptocurrency storage[29].

Within a permissionless environment, all the peers of the network are equally responsible. As a result, should there are losses due to e.g., a failure in the code, the legal liability is undetermined and nobody is held accountable or responsible. What this means is that there is no way to recover the said losses[31]. This is further exacerbated by the fact that, to date, the question of whether cryptocurrencies are money, commodities or something else is still unresolved, and as such, remain fairly unregulated with regulatory bodies, institutional mechanisms and the likes, removed from the payment and storing process. In addition, regulatory and legal frameworks often necessitate the application of some additional layers of control, which, in the case of the Bitcoin, may not be applicable or feasible[32].

Permissioned blockchain

Permissioned blockchains offer a more controlled environment for transactional information. a permissioned environment, the blockchain is developed, used and controlled by a group of participants, or a consortium. As a result, in such cases, trust exists within a set number and

identified parties, and the central assumption that the chain must remain operational and trusted still holds. However, as in the case of a permissionless chain, the novelty of the technology, coupled with the limited (controlled) number of peers being able to see the code, suggests that the code may be insufficiently tested, and the risk of unidentified bugs and vulnerabilities is even greater, and therefore, more prone to malicious attacks and system errors[33].

Permission is granted by the governing parties. These operators need to grant permissions to trusted nodes, who will then take care of the verification process. This means that a risk emerges as a result of granting incorrect permissions. Furthermore, it is expected that there will be fewer nodes responsible for maintaining the network. As such, a single node that restricts the transmission of information, transmits incorrect information, or simply goes offline due to technical issues, suggests that each and every node holds greater responsibility for the health of the network, and that of the chain[34].

Next, some risks of permissioned blockchains relate to their interoperability. It is only natural that each private, permissioned blockchain will operate using a different protocol, and that their implementation will be different. This will result in different models for data and data storage, permission controls and obviously confidentiality. In turn, such differences can lead to complications as the fragmented nature of data residing in private blockchains will make them impossible to later link together[35].

However, we consider that the most critical risk for permissioned blockchains surfaces as a result of using third-party applications. Despite that the blockchain has been proposed as a solution towards increasing the security of cloud-based applications and alleviate any vulnerabilities[36], it is still sensitive to attacks and as secure as its weakest point, which is, in this case, the third-party provider. Most firms and organisations turn to specialised external providers in order to leverage their expertise and build their IT solutions. When IT is outsourced partially or entirely to an external vendor[37], the security of the blockchain will be no greater than the trustworthiness of the chosen vendor. If the vendor has weak security in their own systems, then these will affect the organisation as well and may result in exposing data, credentials and keys to unauthorised entities.

Finally, like other technologies, the blockchain operates within a less controlled environment, standards-wise. The lack of standards suggests that each company, consortium or services operates using a different set of rules. In addition, the blockchain is rarely used on its own; instead, it is often coupled with other concepts and technologies, such the internet of things, cloud computing etc. As a result, it may be unknown what sorts of risks actually exist at the intersection of such technologies, as there doesn't exist a common framework for developing and implementing any single security management practice for blockchain and decentralised applications, nor that there is some baseline approach for maintaining minimum controls over the blockchain solutions. In other words, blockchain developers cannot benefit from the mistakes of others, as there doesn't exist a protocol for documenting and reporting incidents[38].

MAPPING THE BLOCKCHAIN AGAINST SECURITY STANDARDS

In this section, we document existing standards and regulatory frameworks that relate to information security and areas, within which the blockchain seems particularly popular (such as finance and healthcare). We do so in an effort to better understand what the lack of standards may possibly mean for security purposes, as well as to later draw some recommendations, in the form of guidelines for developing blockchain-based applications.

Most importantly, we further identify the applicability of the existing standards and regulations with respect to areas of interest within the blockchain.

Table 1 provides a summary of standards and regulatory frameworks that are pertinent to the Blockchain technology. We present the standards and regulatory frameworks that relate to the Blockchain technology, without having been developed specifically for it. Within this group there are different standards, regulations and acts that blockchain platform providers should consider for industry specific compliance requirements. For example, it includes FIPS 140-2, which details the necessary security guidelines for a cryptographic module and elaborates on the security and storage of cryptographic keys, which are relevant for blockchain applications[39]. Similarly, the Computer Misuse Act has been put together in order to protect IT artefacts from distributed denial of service (DDoS) attacks, which can affect the blockchain[40]. There are several standards and regulations that can be applicable within the blockchain context. However, arguably, the most important one is the newly introduced General Data Protection Regulation (GDPR), which is counterintuitive to the append-only nature of the blockchain. However, following GDPR if an individual demands the deletion or amendment of their personal data, the firm needs to comply[41].

The next group of standards and regulations pertain to areas that exhibit an interest about the technology, such as the financial and the health sectors. Within these two contexts, the blockchain can support increased compliance and provide the necessary monitoring tools. Some of the relevant regulations are naturally the Sarbanes-Oxley Act of 2002, where the blockchain can assist companies with the traceability and the appendability (but not amendability and deletion) of records. Equally important is the Health Insurance portability and accountability act, which details the importance and the processes for maintaining security and privacy. Within the finance sector, the Gramm-Leach-Bliley Act (1999)[42] requires that financial institutions are transparent as far as information sharing is concerned and further documents the responsibility of the said institutes for safeguarding such data. In such cases, the blockchain has the potential to assist with compliance with the Gramm-Leach-Bliley act, since it is a secure ledger that monitors and documents all transactional requests.

Currently no standard has been designed and introduced specifically for the blockchain technology, with the exception of ISO/TC 307, which presently is still under development. Its aim is to bring together different elements of the blockchain and to standardise distributed ledger and blockchain technologies (smart contracts, governance and interoperability issues)[11].

[Table 1 aboute here]

CASE STUDIES: ROOT CAUSE ANALYSIS OF SECURITY INCIDENTS IN THE BLOCKCHAIN ERA

This section analyses the blockchain-related incidents using the case study method[43]. We review publicly available incidents and perform an in-depth analysis of six representative cases out of 38 known incidents. Table 2 presents an overview of our findings. Our aim is to support potential adopters to learn from existing errors and avoid similar pitfalls with this technology that is still in its infancy.

[Table 2 about here]

An overview of blockchain security incidents

We identified and reviewed 38 incidents with the aim to recognise the main root cause (Table 3, Appendix). We classified them into seven root cause categories (Figure 2). The classification is adapted from Li et al.'s[10] classification of Blockchain security causes, enriched by adding insider threat dimensions that have attracted the attention of the community[44]. Half of the incidents occurred due to server or application related vulnerabilities. Others related to insider threats, protocols, and the cloud platform the blockchain ran on. For some incidents, the root causes are still unknown.

[Figure 2 about here]

We selected six incidents for in-depth analysis. The selection is based on the frequency of the root cause. In particular, we look at the issues of server/infrastructure incidents, application vulnerability/smart contract incidents and cloud platform incidents, which account for over 60% of the total number of incidents. The selection also considers the comprehensiveness and reliability of the information sources regarding the incidents. The selected incidents are well documented with enough details to analyse and are from reliable sources such as peer review publications (see Table 2). In what follows we explore the root causes of blockchain incidents in more detail and discuss how they could have been prevented. For each incident, the following questions are addressed: What happened and how? Could damage have been reduced or mitigated and how?

Case 1: The DAO (Application Vulnerability/Smart Contract Code Error)

In June 2016, the Decentralized Autonomous Organization (The DAO) had US $50mn stolen[45]. The DAO was a venture capital fund in the cryptocurrency software industry and had no leader or board and was not associated with any country. The aim of The DAO was to deliver a new business model for organising enterprises. It was a virtual organisation initiated within a smart contract on the Ethereum blockchain. The contract maintains a rule set that allows the capability for contributors to vote on which ventures and projects to fund using the cryptocurrency Ether. Participants who contributed larger amounts during the creation of the DAO are given a proportionally larger number of votes. Once a vote is completed, the Ether cryptocoins are distributed to the venture's cryptowallet and the transaction is recorded on the Ethereum blockchain.

The attack that occurred was facilitated by a software vulnerability identified in the 'split' function. The function was created to let participants of the DAO perform a balance transfer into what was called a 'Child DAO', essentially a new DAO, should they want to move their investments following a vote. The process was as follows; the network confirms the participants account balance, then transfers it to the new DAO, only then is the balance in the original DAO set to zero. This in practice was working correctly, however it was determined that participants could execute another 'split' before the balance was set to zero, and hence perform the same split multiple times to drain the DAO of its value. In the incident a split was executed nearly two hundred times by the hackers. The attack took advantage of the way the blockchain works and of the poor design of the smart contract.

This type of attack could have been avoided had the smart contract code received an exhaustive formal review and assessment before being implemented. The DAO was delisted from trading on the major exchange Poloniex in September 2016 and Kraken in December

2016[45]. This case raises questions around the lack of safeguards in place to ensure blockchain technology is utilised correctly.

Case 2: Bitfinex (Server/Infrastructure Breach)

In August 2016, nearly 120,000 Bitcoin (over US $60mn at the time) were stolen from Bitfinex[45]. Based in Hong Kong, Bitfinex is one of the world's largest digital and cryptocurrency exchanges. Bitfinex operated several security measures, which included a multi-signature key management system that split private keys for each customer's wallet between several parties with the aim of reducing the chance of a successful breach. In this specific case, one key was secured by the third party BitGo, a wallet provider, whilst further two were maintained internally by Bitfinex. To make a transaction all three keys would be required.

There was much debate as to whether the breach was the fault of Bitfinex or Bitgo, however, regardless of where the root cause lay, systematic controls to prevent and detect analogous transactions put into place by either party could have helped lessen the losses sustained. For example, controls that would prevent Bitgo from signing off a transaction simply because Bitfinex had. Bitgo reported no breaches but came under fire for blindly signing off transactions[45].

The incident exploited security vulnerabilities within individual organizations. The blockchain network itself remained fully functional and operated as envisioned. The incident may have been prevented had there been a detailed end-to-end review of security, using scenarios, meaning there would have been a higher chance of identifying risks up front and being able to mitigate them at that point.

Case 3: Coindash (Server/Infrastructure Breach)

In July 2017, over seven million US dollars' worth of Ethereum cryptocurrencies were stolen by hackers from investors in the Israel-based start-up CoinDash[46]. CoinDash considers itself as a platform for managing and trading crypto assets. People buy virtual tokens from CoinDash, as these tokens are supposed to increase in value as the start-up grows. Unfortunately, CoinDash suffered a hacking attack during its Token Sale event, and a fake twitter account (@Coindash_ico) was set up to promote the Token Sale.

The attack occurred during the initial coin offering; the Ethereum address where investments should have been sent was changed to the hackers' own wallet. This was executed by the attackers hacking the Coindash website. The victims were refunded; however, the criminals were not identified which is a common occurrence in blockchain related incidents[47]. The theft was believed to have been initiated by an insider. However, necessary protection on the website, such as network-based threat detection and mitigation[48] could have prevented this attack. In addition, monitoring for malicious insiders could have reduced the likelihood of an insider breach[49].

Case 4: Parity (Application Vulnerability/Smart Contract Code Error)

In November 2017, a smart contract vulnerability in the library code, deployed as a shared component of all multi signature wallets provided by Parity Technologies was identified by an anonymous user[50]. The user was able to make themselves the owner of the library contract. The component was then destroyed, freezing funds in 587 wallets holding over $500,000 in Ether as well as other tokens.

The original multi-signature wallet was created and audited by Ethereum's DEV team, Parity Technologies and others in the community. The code went through an extensive peer review and still showed no known security vulnerabilities. However, the Parity team restructured the

code into a lightweight version that was getting deployed every time a new wallet was created together with a heavier version known as the library element, which was deployed just once and contained most of the logic. When doing this, only few changes were made to create the lighter code and the library code. This meant the library contract still had similar functionality as a regular wallet and required initialisation and still contained the function 'self-destruct' that was supposed to be used for retiring the wallet. No formal audit was made of this library code. Following the attack, the library contract was fixed and re-deployed the next day.

Parity Technology suggested that if the code had not contained the self-destruct function and someone had taken ownership of the library by initialising it (as seen in the actual attack), then there would be no further vulnerability to exploit. The other option would have been for the wallet initialisation to be done automatically through the code change and redeployment or manually when the contract was first deployed so that Parity became the owner. Either way, the vulnerability is that the code was used for a purpose other than that for which it was audited.

Parity Technologies believes that more extensive and formal procedures and tooling around the deployment, monitoring and testing of contracts will be needed to achieve security. This is of greater necessity when the number and complexity of live contracts is growing[50].

Case 5: Zerocoin (Application Vulnerability/Smart Contract Code Error)

In February 2017, a programming error in the Zerocoin implementation was exploited, allowing an attacker to generate multiple spends they could send to an exchange, which were then sold and withdrawn[51]. The Zerocoin protocol consists of minting and spending. Minting a coin means making a coin no longer spendable by 'burning' it. Spending a Zerocoin means redeeming a new coin that has no transaction history. To prove that one is eligible to spend Zerocoin, they must demonstrate that they have minted an equivalent number of coins. The proof only shows that one burnt coins not whether these coins have been redeemed. A unique serial number is generated during the mint phase and posted during the spend phase. Miners verify that the serial number has not been used before and it was this validation phase where the bug lay. In this case, the company identified that the total Zerocoin spent did not align with the total Zerocoin minted during a check to monitor usage. The spent tally in fact far exceeded that of the mint tally. The development team identified that a serial number for a spend transaction had been re-used. The duplicate serial numbers should have been rejected, instead the hacker manage to exploit the single proof.

Investigation by developers revealed that the issue was '==' being used instead of '='. The double equals is a comparison operator, returning a true or false value whereas the single equals makes the first parameter equal to the parameter/value after the equals. This allowed to break the serial code validation. The attacker was immediately sending the created spent transactions to an Altcoin exchange address. Zerocoin then attempted to work with Altcoin to freeze the accounts, however it was too late as the funds had already been sold and withdrawn. Over sixty accounts were used to make it difficult to detect what was happening.

Zerocoin contacted major mining pools asking them to suspend processing any Zerocoin transactions. Some pools were slow to react, resulting in further Zerocoin spent transactions being completed in this windo[51].

This case highlights the importance of routine code reviews as well as internal and external audits. Automated checking systems could also be used to detect exploits as early as possible. There was also no formal process or agreement with the mining pools. If there was an agreed

procedure in emergencies, then perhaps they could have closed the pools earlier, limiting the damage.

Case 6: Inputs.IO Hack (Cloud Platform)

In 2013, hackers stole over 4,000 bitcoins through two separate attacks in the same week from Inputs.Io, a company that stores customers' cryptocurrencies in digital wallets[52]. This was possible through a breach in the cloud infrastructure. In addition, several e-mail accounts were compromised, leading to the attacker being able to reset the password for the Linode Server. Inputs.Io did not have the funds to pay back customers in full.

RECOMMENDATIONS

Based on the increasing use of blockchain technologies and the incidents reviewed, we propose a framework of best practices to reduce the chance of cyber security vulnerabilities. This framework provides solutions for the interactions surrounding blockchain as opposed to altering the technology itself. As explored in previous sections, blockchain technology itself is not usually compromised; instead vulnerabilities arise due to its improper use. We further provide security recommendations for both providers and consumers of the blockchain technology.

Regulatory Compliance - Blockchain solutions are often implemented on cloud platforms, and we have already seen hacks due to the cloud infrastructure (see Figure 2). Stakeholders need to carefully investigate the risks of the cloud platform itself[54], and ensure they choose an appropriate platform to host permissioned blockchains, especially within a regulated industry. Blockchain providers need to ensure their cloud infrastructures are at least compliant with ISO 27001 and ISO 270017. Blockchain consumers dealing with personally identifiable information (PII) should also ensure their providers are compliant with ISO 270018. This will help ensure that the necessary security controls are in place. Blockchain providers should also consider industrial specific compliance requirements. In the healthcare industry, platforms should be built with compliance to country specific acts, such HIPAA. This allows adopters to meet the needs of the industry more easily keeping patient data secure. In the finance industry, there are also platforms on offer, such as IBM Blockchain framework[55], to help with compliance with FISMA, SOX and Gramm Bleach Bliley.

Blockchain Providers Selection - Blockchain consumers should carefully consider platforms available when choosing a third-party provider. The question they should ask is: will this provider help me to be compliant with the needs of my industry? Likewise, Blockchain providers need to have the consumer in mind by ensuring that their blockchain frameworks contain detailed guidance on how they can help consumers to satisfy their industrial needs. Good practices are the IBM and Microsoft blockchain frameworks[55,56] that specify their country specific and industrial specific standards that they have addressed and also provide considerations that the consumer must undertake to avoid security breaches. In essence, a successful blockchain framework must inform an organisation to select a provider that meets all their needs.

Routine Audits – Ou reivew flagged the need for formal reviews of all smart code contracts. Mistakes can compromise the entire system as seen with The DAO incident[45]. The blockchain framework should contain detail of how an internal formal code review should be carried out[57], and who should carry out the review, what experience is required to undertake the review and what seniority level is required for sign off. This may vary between industry sectors. Details should be provided on how often external reviews should take place. It is unrealistic for all smart code contracts to be externally audited, however all should go through detailed internal reviews. The framework should also state that if a code has been

audited for a specific purpose, it should not be used for other purposes. Using the code in an alternative way would constitute the need for another review for the new suggested purpose. This would have helped mitigate the Parity Vulnerability review[50]

Automation of Blockchain Incident Response - We identified the need for a formal process to be agreed upon by communities for incident response. In the case of the Zerocoin hack, if there were an automated way to inform mining pools about the incident, activities could have been suspended until fixed[51]. This example is specific to the cryptocurrency world; however, automation of blockchain incident response should be considered in all other industries. Furthermore, in the root cause analysis, it was noted that in many cases the root causes of hacks were not discussed or recorded. This results in a lack of ability for the wider blockchain community to learn from security breaches. Companies can therefore fall victim to the same attacks that could otherwise have been prevented. Therefore, it is recommended that mandatory public information sharing is necessary at the earliest opportunity. This will also allow other organisations adopting the technology to learn from other communities, as although their purpose in using the blockchain may be different, the vulnerabilities remain the same.

Use of Hot Wallets and Cold Wallets - Hot wallets were identified earlier as a key risk, with some incidents being the result of hackers gaining access to hot wallets. Although the vulnerability may have been elsewhere, if cold storage had been used, the attack could have been mitigated. This is not to say that cold storage is completely secure, but we have seen many more hot wallet breaches in comparison to cold storage (see Figure 2). Therefore, it is recommended that keys of value are stored using cold storage methods. It would be difficult to eradicate the use of hot wallets as they aid the efficiency of transactions, however the data stored in hot wallets should be strongly considered prior to use. It is suggested that major exchanges should keep most funds in cold storage[10].

End-to-end Product Life Cycle Reviews - Detailed end-to-end reviews should be part of the business process to try and identify vulnerabilities through risk-based scenarios. This would aid proactive identification of risk rather than waiting until they materialise. There is limited research in blockchain risk management in the product life cycle review. Experience can be borrowed from cyber security risk assessment (Rauter, et, al., 2016) that key blockchain risk factors throughout the product life cycle should be identified, measured, prioritised and mitigated (e.g. avoiding, minimising, transferring or containing) to an acceptable level that is benchmarked or predefined.

Automated Checks - Where possible automated checks[58] should be in place to ensure the systems and processes are working as expected. For example, in the Zerocoin incident, if they had noticed that total Zerocoin spend did not align with the total Zerocoin minted earlier, the amount stolen would have been much less (Insom, 2017). In this respect, 'Automated Management Information Reports' could be designed to check such totals and send an alert when a mis-match is detected.

CONCLUSIONS AND FUTURE WORK

The Blockchain is designed to be secure and the technology has great potential benefits. However, through the interactions with software systems, web-based systems, clouds and other platforms, security risks can be introduced to Blockchain systems. It must be used appropriately with the use of a security framework. Currently, businesses and organisations operate under a lack of standards. Based on an extensive review of the existing standards and regulations, we identified their applicability that is connected to Blockchain. The incidents reviewed highlight key points that should be included in a blockchain specific framework,

including regulatory compliance, Blockchain provider selection, the need for thorough smart contract code reviews and both internal and external audits, the automation of incident response methods and checks, appropriate use of cold storage techniques where possible and end-to-end product life cycle reviews and automated checks. Our intention is not to provide an all-encompassing framework, but to highlight ways for identifying, exploring and addressing risks related to Blockchain technology. This also contributes to the creation of the Blockchain specific security standard regarding what security concerns need to be included and addressed. One limitation of this work is that the derived root causes and recommended security solutions have not been scientifically verified or executed in experiments. Future work should improve on this by verifying the framework through experimentation. Future work will be focusing on the elaboration of the above-mentioned seven aspects within the framework and borrow experience from general information security area including regulatory compliance, risk assessment, incident response, access control, auditing and contingency planning.

REFERENCES

1. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Nakamoto Institute. 2008.

2. Psaila S. Blockchain: A game changer for audit processes? Deloitte Malta; 2018. Audit & Assurance. https://www2.deloitte.com/mt/en/pages/audit/articles/mt-blockchain-a-game-changer-for-audit.html

3. Nikolic I, Kolluri A, Sergey I, Saxena P, Hobor A. Finding The Greedy, Prodigal, and Suicidal Contracts at Scale. arXiv:1802.06038 [cs]. 2018 Feb 16 [accessed 2018 Jul 11]. http://arxiv.org/abs/1802.06038

4. 360TS. 360 Discovered an Epic BlockChain Vulnerability in EOS and All Transaction Can Be Manipulated. 360 Total Security Blog. 2018 May 29 [accessed 2018 Jul 11]. https://blog.360totalsecurity.com/en/360-discovered-epic-blockchain-vulnerability-transaction-can-manipulated/

5. Tosh DK, Shetty S, Liang X, Kamhoua CA, Kwiat KA, Njilla L. Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack. IEEE; 2017. p. 458–467. http://ieeexplore.ieee.org/document/7973732/.

6. Rizzo P. Hackers Steal Over $300k From One of Blockchain's Biggest VCs. CoinDesk. 2016 Dec 6 [accessed 2018 Jul 11]. https://www.coindesk.com/hackers-stole-300k-blockchain-investor/

7. Luu L, Chu D-H, Olickel H, Saxena P, Hobor A. Making Smart Contracts Smarter. ACM Press; 2016. p. 254–269. http://dl.acm.org/citation.cfm?doid=2976749.2978309. doi:10.1145/2976749.2978309

8. Atzei N, Bartoletti M, Cimoli T. A Survey of Attacks on Ethereum Smart Contracts (SoK). In: Maffei M, Ryan M, editors. Principles of Security and Trust. Vol. 10204. Berlin, Heidelberg: Springer Berlin Heidelberg; 2017. p. 164–186.

9. Zimba A, Wang Z, Mulenga M, Odongo NH. Crypto Mining Attacks in Information Systems: An Emerging Threat to Cyber Security. Journal of Computer Information Systems. 2018 May 31:1–12.

10. Li X, Jiang P, Chen T, Luo X, Wen Q. A survey on the security of blockchain systems. Future Generation Computer Systems. 2017 Aug [accessed 2018 Jul 11]. http://linkinghub.elsevier.com/retrieve/pii/S0167739X17318332.

11. ISO. Blockchain and distributed ledger technologies. 2016. Report No.: ISO/TC 307. https://www.iso.org/committee/6266604.html

12. Xu X, Weber I, Staples M, Zhu L, Bosch J, Bass L, Pautasso C, Rimba P. A Taxonomy of Blockchain-Based Systems for Architecture Design. IEEE; 2017. p. 243–252.

13. Luttgens JT, Pepe M, Mandia K. Incident Response & Computer Forensics. 3rd ed. McGraw-Hill Education Group; 2014.

14. Zamani ED, Giaglis GM. With a little help from the miners: distributed ledger technology and market disintermediation. Industrial Management & Data Systems. 2018;118(3):637–652.

15. Conti M, E SK, Lal C, Ruj S. A Survey on Security and Privacy Issues of Bitcoin. IEEE Communications Surveys & Tutorials. 2018:1–1.

16. Lu Q, Xu X. Adaptable Blockchain-Based Systems: A Case Study for Product Traceability. IEEE Software. 2017;34(6):21–27.

17. Okada H, Yamasaki S, Bracamonte V. Proposed classification of blockchains based on authority and incentive dimensions. IEEE; 2017. p. 593–597.

18. Swan M. Blockchain for Business: Next-Generation Enterprise Artificial Intelligence Systems. In: Advances in Computers. Elsevier; 2018. http://linkinghub.elsevier.com/retrieve/pii/S0065245818300287.

19. O'Leary D. Configuring blockchain architectures for transaction information in blockchain consortiums: The case of accounting and supply chain systems. Intelligent Systems in Accounting, Finance and Management. 2017;24(4):138–147.

20. Killmeyer J, White M, Chew B. Will blockchain transform the public sector? Blockchain basics for government. Deloitte University Press; 2017. https://www2.deloitte.com/content/dam/insights/us/articles/4185_blockchain-public-sector/DUP_will-blockchain-transform-public-sector.pdf

21. Peck ME. Why the Biggest Bitcoin Mines Are in China. IEEE Spectrum. 2017 Oct 4 [accessed 2018 Jun 11]. https://spectrum.ieee.org/computing/networks/why-the-biggest-bitcoin-mines-are-in-china

22. Fairley P. Blockchain world - Feeding the blockchain beast if bitcoin ever does go mainstream, the electricity needed to sustain it will be enormous. IEEE Spectrum. 2017;54(10):36–59.

23. Efanov D, Roschin P. The All-Pervasiveness of the Blockchain Technology. Procedia Computer Science. 2018;123:116–121.

24. Naheem MA. Regulating virtual currencies - the challenges of applying fiat currency laws to digital technology services Futter A, editor. Journal of Financial Crime. 2018 Mar 6:00–00.

25. Hsu S. China's Shutdown Of Bitcoin Miners Isn't Just About Electricity. Forbes. 2018 Jan 15 [accessed 2018 Jun 12]. https://www.forbes.com/sites/sarahsu/2018/01/15/chinas-shutdown-of-bitcoin-miners-isnt-just-about-electricity/#6836c806369b

26. Xu JJ. Are blockchains immune to all malicious attacks? Financial Innovation. 2016;2(1):25.

27. Mokoena T, Zuva T. Malware Analysis and Detection in Enterprise Systems. IEEE; 2017. p. 1304–1310.

28. Zhang R, Preneel B. Publish or Perish: A Backward-Compatible Defense Against Selfish Mining in Bitcoin. In: Handschuh H, editor. Topics in Cryptology – CT-RSA 2017. Vol. 10159. Cham: Springer International Publishing; 2017. p. 277–292.

29. He S, Wu Q, Luo X, Liang Z, Li D, Feng H, Zheng H, Li Y. A Social-Network-Based Cryptocurrency Wallet-Management Scheme. IEEE Access. 2018;6:7654–7663.

30. Biggs J. A 15-year-old hacked the secure Ledger crypto wallet. TechCrunch. 2018 [accessed 2018 Jun 18]. http://social.techcrunch.com/2018/03/21/a-15-year-old-hacked-the-secure-ledger-crypto-wallet/

31. Tu KV, Meredith M. Rethinking Virtual Currency Regulation in the Bitcoin Age. Washington Law Review. 2015;90:271–347.

32. Burge ME. Apple Pay, Bitcoin, and Consumers: The ABCs of Future Public Payments Law. Hastings Law Journal. Texas A&M University School of Law Legal Studies. 2015;67:1493–1550.

33. van Deventer O, Berkers F, Vos M, Zandee A, Vreuls T, van Piggelen L, Blom A, Heeringa B, Akdim S, van Helvoort P, et al. Techruption Consortium Blockchain – what it takes to run a blockchain together. In: 1st ERCIM Blockchain Workshop 2018. Vol. 2, no 9. 2018.

34. Berke A. How Safe Are Blockchains? It Depends. Harvard Business Review. 2017 Mar 7 [accessed 2018 Jun 18]. https://hbr.org/2017/03/how-safe-are-blockchains-it-depends

35. Guardian Analytics. The Risks of Private Blockchain: Too Many. Guardian Analytics. 2017 [accessed 2018 Jan 16]. https://guardiananalytics.com/risks-of-private-blockchain-too-many-chains/

36. Singh I, Lee S-W. Comparative Requirements Analysis for the Feasibility of Blockchain for Secure Cloud. In: Kamalrudin M, Ahmad S, Ikram N, editors. Requirements Engineering for Internet of Things. Vol. 809. Singapore: Springer Singapore; 2018. p. 57–72.

37. Lee J. Strategic risk analysis for information technology outsourcing in hospitals. Information & Management. 2017;54(8):1049–1058.

38. von Solms R. Information security management: why standards are important. Information Management & Computer Security. 1999;7(1):50–58.

39. NIST. FIPS 140-2. 2002 [accessed 2018 Feb 3]. https://csrc.nist.gov/publications/detail/fips/140/2/final

40. UK Government. Computer Misuse Act 1990. 2018 [accessed 2018 Mar 11]. https://www.legislation.gov.uk/ukpga/1990/18/contents

41. European Commission. EUR-Lex - 52018DC0043 - EN - EUR-Lex. 2018 [accessed 2018 Jun 19]. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043

42. US Congress. GRAMM–LEACH–BLILEY ACT. 1999. Report No.: Public Law 106-102.

43. Gillham B. Case Study Research Methods. Bloomsbury Publishing; 2000.

44. Tasca P, Tessone CJ. Taxonomy of Blockchain Technologies. Principles of Identification and Classification. Univesity College London; 2017. http://arxiv.org/abs/1708.04872

45. Nagaraj K, Maguire E. Securing the Chain. KPMG International; 2017. kpmg.com/blockchain360. https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/05/securing-the-chain.pdf

46. Jabotinsky HY. The Regulation of Cryptocurrencies - Between a Currency and a Financial Product. SSRN Electronic Journal. 2018 Feb 7 [accessed 2018 Jul 11]. https://papers.ssrn.com/abstract=3119591

47. Leyden J. CoinDash crowdfunding hack further dents trust in crypto-trading world. The Register. 2017 Jul 18 [accessed 2018 Jul 11]. https://www.theregister.co.uk/2017/07/18/coindash_hack/

48. Amsler DB, Allen N, Messer S, Healy T. Automated internet threat detection and mitigation system and associated methods. 2016 Feb 9 [accessed 2018 Jul 11]. https://patents.google.com/patent/US9258321B2/en

49. Omar M. Insider Threats: Detecting and Controlling Malicious Insiders. In: New Thretas and Countermeasures in Digital Crime and Cyber Terrorism. IGI Global; 2015. p. 162–172. https://www.igi-global.com/chapter/insider-threats/131402

50. Parity Technologies. A Postmortem on the Parity Multi-Sig Library Self-Destruct. ParityTech. 2017 Nov 15 [accessed 2018 Jul 13]. https://paritytech.io/a-postmortem-on-the-parity-multi-sig-library-self-destruct/

51. Insom P. Zcoin's Zerocoin bug explained in detail. Zcoin. 2017 [accessed 2018 Jul 13]. https://zcoin.io/zcoins-zerocoin-bug-explained-in-detail/

52. McMillan R. $1.2M Hack Shows Why You Should Never Store Bitcoins on the Internet. Wired. 2013 Nov 7 [accessed 2018 Jul 16]. https://www.wired.com/2013/11/inputs/

53. Inayat Z, Gani A, Anuar NB, Anwar S, Khan MK. Cloud-Based Intrusion Detection and Response System: Open Research Issues, and Solutions. Arabian Journal for Science and Engineering. 2017;42(2):399–423. doi:10.1007/s13369-016-2400-3

54. Choi J, Nazareth DL, Ngo-Ye TL. The Effect of Innovation Characteristics on Cloud Computing Diffusion. Journal of Computer Information Systems. 2018;58(4):325–333. doi:10.1080/08874417.2016.1261377

55. Gautham. IBM Announces Security Focused Blockchain Framework. NewsBTC. 2016 [accessed 2018 Jul 16]. https://www.newsbtc.com/2016/05/03/ibm-announces-security-focused-blockchain-framework/

56. Microsoft. Microsoft helps launch world's first blockchain-based investment product. Microsoft News Centre UK. 2018 [accessed 2018 Jul 16]. https://news.microsoft.com/en-gb/2018/03/21/microsoft-azure-helps-nivaura-launch-worlds-first-blockchain-based-investment-product/

57. Bharadwaj K. Blockchain 2.0: Smart Contracts. linkĐapps. 2016 [accessed 2018 Jul 16]. http://www.linkdapps.com/Blockchain2.0-SmartContracts.pdf

58. Fridgen G, Radszuwill S, Urbach N, Utz L. Cross-Organizational Workflow Management Using Blockchain Technology - Towards Applicability, Auditability, and Automation. In: 51st Hawaii International Conference on System Sciences (HICSS 2018). Waikoloa Village, Hawaii; 2018.

59. IT GOVERNANCE. PAS 555 2013 Cyber Security Risk Governance and Management Specification. 2013 [accessed 2018 Jan 11]. https://www.itgovernance.co.uk/shop/product/pas-555-2013-cyber-security-risk-governance-and-management-specification

60. IEEE. IEEE Std C37.240-2014 – IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems. 2014 [accessed 2018 Jan 14]. https://standards.ieee.org/findstds/standard/C37.240-2014.html

61. COMMON CRITERIA. Common Criteria for Information Technology Security Evaluation. 2012 [accessed 2018 Feb 6]. http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf

62. Congress.Gov. S.2521 - Federal Information Security Modernization Act of 2014. Congress.Gov. 2014 Jun 24 [accessed 2018 Jan 19]. https://www.congress.gov/bill/113th-congress/senate-bill/2521

63. IT GOVERNANCE. ISO 27001, the international information security standard. 2017 [accessed 2017 Dec 10]. https://www.itgovernance.co.uk/iso27001

64. ISO. ISO/IEC 27005:2011 - Information technology -- Security techniques -- Information security risk management. 2011 [accessed 2018 Jun 19]. https://www.iso.org/standard/56742.html

65. ISO. ISO/IEC 27017:2015 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services. 2015 [accessed 2018 Jun 19]. https://www.iso.org/standard/43757.html

66. ISO. ISO/IEC 27018:2014 - Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. 2014 [accessed 2018 Jun 19]. https://www.iso.org/standard/61498.html

67. SOXLAW. The Sarbanes-Oxley Act 2002. 2006 [accessed 2018 Jun 19]. http://www.soxlaw.com/

68. King M. Reinventing reconciliation with Blockchain technology. 2016 [accessed 2018 Jun 19]. https://www.greshamtech.com/blog/reinventing-reconciliation-with-blockchain-technology

69. Office for Civil Rights (OCR). Summary of the HIPAA Privacy Rule. HHS.gov. 2008 May 7 [accessed 2018 Jun 19]. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

70. Zhang P, Schmidt DC, White J, Lenz G. Blockchain Technology Use Cases in Healthcare. In: Advances in Computers. Elsevier; 2018. http://linkinghub.elsevier.com/retrieve/pii/S0065245818300196. doi:10.1016/bs.adcom.2018.03.006

71. Accenture. Editing the Uneditable Blockchain. Why distributed ledger technology must adapt to an imperfect world. 2016. https://www.accenture.com/t20160927T033514Z__w__/ae-en/_acnmedia/PDF-33/Accenture-Editing-Uneditable-Blockchain.pdf

72. Kalkan K, Kwansa F, Cobanoglu C. Payment Card Industry Data Security Standards (PCI DSS) Compliance in Restaurants. Journal of Hospitality Financial Management. 2010;6(2).

73. DuPont Q. Experiments in algorithmic governance : A history and ethnography of “The DAO,” a failed decentralized autonomous organization. Bitcoin and Beyond (Open Access). 2017 Nov 28 [accessed 2018 Oct 12].

74. Miers I, Garman C, Green M, Rubin AD. Zerocoin: Anonymous Distributed E-Cash from Bitcoin. IEEE; 2013. p. 397–411.

75. Osborne C. Bitcoin exchange Cryptoine hacked | ZDNet. ZDNet. 2015 Mar 26 [accessed 2018 Oct 12]. https://www.zdnet.com/article/bitcoin-exchange-cryptoine-hacked/

76. DeMartino I. CryptoThrift Suffers Security Breach, 15 BTC Stolen, Escrow Service Suspended. Cointelegraph. 2014 Oct 7 [accessed 2018 Oct 12]. https://cointelegraph.com/news/cryptothrift-suffers-security-breach-15-btc-stolen-escrow-service-suspended

77. Rizzo P. Poloniex Loses 12.3% of its Bitcoins in Latest Bitcoin Exchange Hack. Coindesk. 2014 Jun 3 [accessed 2018 Oct 12]. https://www.coindesk.com/poloniex-loses-12-3-bitcoins-latest-bitcoin-exchange-hack/

78. Hern A. Bitcoin bank Flexcoin closes after hack attack. the Guardian. 2014 Apr 3 [accessed 2018 Oct 12]. https://www.theguardian.com/technology/2014/mar/04/bitcoin-bank-flexcoin-closes-after-hack-attack

79. Redman J. The Bitcoin Exchange Thefts You May Have Forgotten. Bitcoin News. 2017 [accessed 2018 Oct 12]. https://news.bitcoin.com/bitcoin-exchange-thefts-forgotten/

80. Altcoin News. [Another] Crypto Wallet Hack Sees Theft of $400,000 in Stellar Lumens. CCN. 2018 Jan 15 [accessed 2018 Oct 12]. https://www.ccn.com/yet-another-crypto-wallet-hack-causes-users-lose-400000/

81. Bradley. Bitcoin mining service “Cloudminr.io” Hacked. Hacker’s List. 2017 [accessed 2018 Oct 12]. https://www.hackers-list.com/bitcoin-mining-service-cloudminr-io-hacked-users-database-sale/

82. Higgins S. Gatecoin Claims $2 Million in Bitcoins and Ethers Lost in Security Breach. CoinDesk. 2016 May 16 [accessed 2018 Oct 12]. https://www.coindesk.com/gatecoin-2-million-bitcoin-ether-security-breach/

83. ShepeShift. A Timeline: ShapeShift Hacking Incident. ShapeShift. 2016 [accessed 2018 Oct 12]. https://info.shapeshift.io/blog/2016/04/19/blog-2016-04-19-timeline-shapeshift-hacking-incident/

84. Buntinx JP. Coinsecure Confirms Victims of Recent Hack Will be Refunded Soon. NewsBTC. 2018 [accessed 2018 Oct 12]. https://www.newsbtc.com/2018/04/17/coinsecure-confirms-victims-recent-hack-will-refunded/

85. Higgins S. Cryptsy CEO Stole Millions From Exchange, Court Receiver Alleges. CoinDesk. 2016 Aug 11 [accessed 2018 Oct 12]. https://www.coindesk.com/cryptsy-ceo-millions-digital-currency-steal/

86. Pick L. Justcoin shutting down today, cites bank account closure, comes weeks after $300k “goxing.” Finance Magnates | Financial and business news. 2014 Oct 29 [accessed 2018 Oct 12]. https://www.financemagnates.com/cryptocurrency/exchange/justcoin-shutting-down-today-cites-bank-account-closure-weeks-after-300k-goxing/

87. Bradbury D. Silk Road 2 Loses Over $2.6 Million in Bitcoins in Alleged Hack. CoinDesk. 2014 Feb 13 [accessed 2018 Oct 12]. https://www.coindesk.com/silk-road-2-loses-bitcoins-hack/

88. Higgins S. Bitcoin Exchange Youbit to Declare Bankruptcy After Hack. CoinDesk. 2017 Dec 19 [accessed 2018 Oct 12]. https://www.coindesk.com/south-korean-bitcoin-exchange-declare-bankruptcy-hack/

89. Russell J. Tether, a startup that works with bitcoin exchanges, claims a hacker stole $31M | TechCrunch. TechCrunch. 2017 Nov 20 [accessed 2018 Oct 12]. https://techcrunch.com/2017/11/20/tether-claims-a-hacker-stole-31m/

90. Allison D. Atlanta’s Bitpay got hacked for $1.8 million in bitcoin. Atlanta Business Chronicle. 2015 Sep 16 [accessed 2018 Oct 12].

https://www.bizjournals.com/atlanta/blog/atlantech/2015/09/atlantas-bitpay-got-hacked-for-1-8-million-in.html

91. Muscat I. Lessons to Learn from the AllCrypt Hack. Acunetix. 2015 [accessed 2018 Oct 12]. https://www.acunetix.com/blog/articles/lessons-to-learn-from-the-allcrypt-hack/

92. Sharwood S. Supposedly secure Dogecoin service Dogevault goes offline. 2014 May 13 [accessed 2018 Oct 12]. https://www.theregister.co.uk/2014/05/13/supposedly_secure_dogecoin_service_dogevault_goes_offline/

93. Securus Global. Bitcoin wallet service suspended following security incident | Securus Global Blog. 2013 [accessed 2018 Oct 12]. https://www.securusglobal.com/community/2013/04/04/bitcoin-wallet-service-suspended-following-security-incident/

94. Dotson K. Bitcoin7 Hacked, Funds Recovery Requires Sensitive Personal Information - SiliconANGLE. 2011 Jul 10 [accessed 2018 Oct 12]. https://siliconangle.com/2011/10/07/bitcoin7-hacked-funds-recovery-requires-sensitive-personal-information/

95. BBC. Biggest ever digital currency "theft." 2018 Jan 27 [accessed 2018 Oct 12]. https://www.bbc.com/news/world-asia-42845505

96. Novak M. NiceHash says attacked probably from non-EU IP address. Reuters. 2017 Dec 8 [accessed 2018 Oct 12]. https://uk.reuters.com/article/us-cyber-nicehash/nicehash-says-attacked-probably-from-non-eu-ip-address-idUKKBN1E21Q7

97. Fincham N. Slush's bitcoin mining pool hacked. MineForeman.com. 2013 Apr 24 [accessed 2018 Oct 12]. https://mineforeman.com/2013/04/24/slushs-bitcoin-mining-pool-hacked/

98. Higgins S. Details of $5 Million Bitstamp Hack Revealed. CoinDesk. 2015 Jul 1 [accessed 2018 Oct 12]. https://www.coindesk.com/unconfirmed-report-5-million-bitstamp-bitcoin-exchange/

99. McMillan R. Hackers Pull Off $12,000 Bitcoin Heist. Wired. 2013 Mar 7 [accessed 2018 Oct 12]. https://www.wired.com/2013/03/digital-thieves-pull-off-12000-bitcoin-heist/

100. Shares D. Names, phone numbers, and emails leaked in BitQuick exchange hack. Bitcoin News. 2016 [accessed 2018 Oct 12]. https://news.bitcoin.com/names-phone-numbers-emails-leaked-bitquick-exchange-hack/

101. Traderman. Coinkite Says "we may have leaked a copy of our database." NullTX. 2016 [accessed 2018 Oct 12]. https://nulltx.com/coinkite-says-we-may-have-leaked-a-copy-of-our-database/

102. Higgins S. Bitcoin Exchange Cointrader Shuts Down After Alleged Hack. CoinDesk. 2016 Mar 30 [accessed 2018 Oct 12]. https://www.coindesk.com/bitcoin-exchange-cointrader-shuts-down/

103. Khandelwal S. Danish Bitcoin exchange BIPS hacked and 1,295 Bitcoins worth $1 Million Stolen. The Hacker News. 2013 Nov 25 [accessed 2018 Oct 12]. https://thehackernews.com/2013/11/danish-bitcoin-exchange-bips-hacked-and_25.html

104. Riley D. Mintpal scammer Ryan Kennedy arrested in U.K. over theft of 3,700 Bitcoins. SiliconANGLE. 2015 [accessed 2018 Oct 12]. https://siliconangle.com/2015/02/23/mintpal-scammer-ryan-kennedy-arrested-in-u-k-over-theft-of-3700-bitcoins/

105. Adamowski J. Polish Bitcoin Exchange Bidextreme.pl Hacked, Bitcoin Wallets Emptied. 2013 Nov 20 [accessed 2018 Oct 12]. https://www.coindesk.com/hacker-attack-polands-bitcoin-exchange/

106. Dotson K. Third Largest Bitcoin Exchange Bitomat Lost Their Wallet, Over 17,000 Bitcoins Missing. 2011 Jan 8 [accessed 2018 Oct 12]. https://siliconangle.com/2011/08/01/third-largest-bitcoin-exchange-bitomat-lost-their-wallet-over-17000-bitcoins-missing/

APPENDIX: BLOCKCHAIN INCIDENTS AND SOURCES

[table 3 about here]

Table 1. Description of pertinent existing standards and regulations

Standard/Regulation/Act	Description/Coverage/Aim	Relation to blockchain
Relevant for Blockchain-based products and services		
Federal Information Processing Standards (FIPS 140-2)[39]	Security needs for a cryptographic module. Published in 2001 and updated in 2002. Specific to United States of America.	Cryptographic keys are a critical element of blockchain technology. FIPS-140-2 looks at security and storage of such items.
Computer Misuse Act (1990)[40]	United Kingdom legislation to protect computers from purposeful attacks and the theft of information.	Distributed Denial of Service (DDoS) attacks on blockchain platforms as well as theft of cryptographic keys are examples of blockchain related items covered by the act.
PAS 555 2013 Cyber Security Risk Governance and Management Specification[59]	International all-inclusive framework for cyber security, setting out technical requirements as well as physical, behavioural and cultural elements.	Not designed specifically for blockchain but can be applied.
IEE std c37.240-2014[60]	International cyber security requirements for substation automation, protection and control systems.	Not designed specifically for blockchain but can be applied.
Common Criteria for Information Technology Security Evaluation (CC v3.1)[61]	International standard that removes redundant evaluation activities that do not contribute significantly to the final assurance of a product	Not specific to blockchain, but applicable when building blockchain based applications or products.
Federal Information Security Management Act 2014 (FISMA)[62]	Comprehensive framework to protect government operations, assets and information from threats. This is United States federal law.	Not directly related to blockchain, but applicable when looking at aspects of information security.
ISO/IEC 27001:2013[63]	International information security management standard that defines best practice for an information security management system.	Can be applied to blockchain technology since it can be thought of as a security management system. The standard could be applied to any part of a business.
ISO/IEC 27005:2011 27005[64]	Supports implementation of ISO/IEC 27001.	As with ISO 27001 it can be applied to blockchain but is not tailor made.
General Data Protection Regulation (GDPR)[41]	Synchronise European data privacy laws, as well as to protect and empower all EU citizens data privacy. Enforceable from 25th May 2018.	GDPR says that people can demand that their personal data is rectified or deleted under several circumstances. This must be a key consideration for blockchain technology where personal data is used as it is essentially a growing record with a traceable history. Therefore, GDPR compliance could be a barrier.
ISO/IEC 27017:2015[65]	Information technology, security techniques and code of practice for information security controls based on ISO/IEC 27002 for cloud services.	Directly related to cloud technology which blockchain platforms can be ran on.
ISO/IEC 27018:2014[66]	Information technology, security techniques and code of practice for protection of personally identifiable information (PII) in public clouds	Specific to PII on Cloud services. Blockchain platforms can be run on cloud services.

	acting as PII processors.	
Regulations that affect areas that can benefit by Blockchain technologies		
Sarbanes-Oxley Act of 2002 (SOX)[67]	Reform corporate financial reporting and accounting. This is United States federal law.	Blockchain has the potential to assist companies with compliance to SOX [68]
Health Insurance Portability and Accountability Act of 1996 (HIPAA)[69]	Security and privacy of specific health data to ensure its protection. This is United States federal law.	Blockchain has potential to assist with HIPAA compliance, improving patient care as well as operational efficiency in the healthcare industry [70]
Gramm-Leach-Bliley Act (1999)[42]	United States Act that requires financial institutes to be clear with their information sharing practices and details the responsibility of the organisation to safeguard sensitive data.	Blockchain has potential to assist with compliance to the act. If crypto currency exchanges get classified as financial institutions, then they would also be obliged to adhere to the cyber security policies and procedures within the Act [71].
Payment Card Industry Data Security Standard (PCI DSS) (2004)[72]	The standard developed consists of twelve requirements created to improve cardholder data security.	Applicable should financial institutions look to move cardholder data onto blockchain networks.
Directly related to the Blockchain		
ISO/TC 307 (In development)[11]	Standardises distributed ledger and blockchain technologies. There are currently 8 ISO standards in the development stage under ISO/TC 307.	Directly related to blockchain, but it is not yet completed. Will cover aspects including Smart contracts, governance and interoperability.

Table 2. Blockchain Incidents Root Causes and Requirements for prevention

Incidents	Incident Type	What are the root causes?	What is required to prevent the incident?
The DAO[45,73]	Application Vulnerability/ Smart Contract Code Error	Software vulnerability in the 'split' function, allowing hackers to run split multi-times to drain the DAO of its value; Poor design of the smart contract	Peer-review and testing of code before deployment Smart contract audits by independent testing facilities
Bitfinex[45]	Server/Infrastructure Breach	Key parties of the multi-signature key management system blindly signing off transactions	Systematic controls to prevent and detect analogous transactions; End to end security review using scenarios
Coindash[46,47]	Server/Infrastructure Breach	Coindash website hack resulting in Ethereum address changed to the hackers' wallet address Suspicious malicious insiders	Web-based attack detection and prevention Defence against malicious insiders
Parity[47,50]	Application Vulnerability/ Smart Contract Code Error	Smart contract vulnerability in the library code; Code containing self-destruct function; Restructured code (light version) not reviewed	Smart contract code review and audits; Formal procedures and tooling for testing complex live smart contracts

Zerocoin[51,74]	Application Vulnerability/ Smart Contract Code Error	A programming error ('==' being used instead of '=') allowing an attacker to duplicate serial numbers and generate multiple spends	Routine code reviews and internal and external audits; Formal agreements and automated procedure in emergent blockchain incident handling
Inputs.IO Hack[52,53]	Cloud Platform	Cloud infrastructure break; Email accounts compromise allowing the attackers to reset the server password Digital wallets breach	Cloud platform security protection; Digital wallets risk management; Considering cold storage for storing keys and crypto currency

Table 3. List of incidents

Incident	Root Cause	Source
The DAO	Application Vulnerability/Smart Contract Code Error	[45]
Zcoin	Application Vulnerability/Smart Contract Code Error	[51]
Cryptoine	Application Vulnerability/Smart Contract Code Error	[75]
Cryptothrift	Application Vulnerability/Smart Contract Code Error	[76]
Poloniex	Application Vulnerability/Smart Contract Code Error	[77]
Flexcoin	Application Vulnerability/Smart Contract Code Error	[78]
Parity	Application Vulnerability/Smart Contract Code Error	[50]
Inputs	Cloud Platform	[52]
Bitcoinica	Cloud Platform	[79]
Black Wallet	Cloud Platform	[80]
Cloudminr	Cloud Platform	[81]
Gatecoin	Cold Storage	[82]
Shapeshift	Insider Threat	[83]
Coinsecure	Insider Threat	[84]
Cryptsy	Insider Threat	[85]
Justcoin	Protocol	[86]
Silk Road 2.0	Protocol	[87]
Youbit	Server/Infrastructure Breach	[88]
Tether	Server/Infrastructure Breach	[89]
Bitfinex	Server/Infrastructure Breach	[45]
Bitpay	Server/Infrastructure Breach	[90]
Allcrypt	Server/Infrastructure Breach	[91]
Dogevault	Server/Infrastructure Breach	[92]
Instawallet	Server/Infrastructure Breach	[93]
Bitcoin7	Server/Infrastructure Breach	[94]
Coincheck	Server/Infrastructure Breach	[95]
Nicehash	Server/Infrastructure Breach	[96]
Coindash	Server/Infrastructure Breach	[47]
Slush's Pool	Server/Infrastructure Breach	[97]

Bitstamp	Social Engineering	98
Bitinstant	Social Engineering	99
Bitquick	Unknown	100
Coinkite	Unknown	101
Cointrader	Unknown	102
Bips	Unknown	103
Mintpal	Unknown	104
Bid Extreme	Unknown	105
Bitomat	Unknown	106

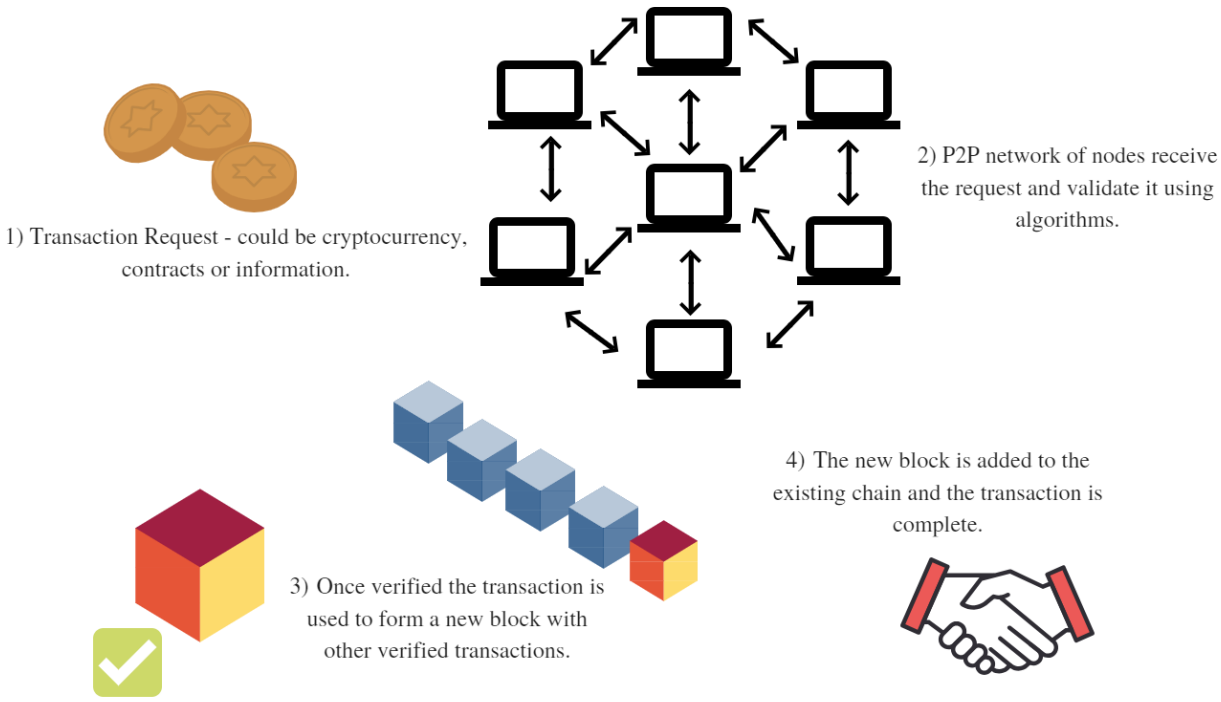

Figure 1. How the Blockchain works.

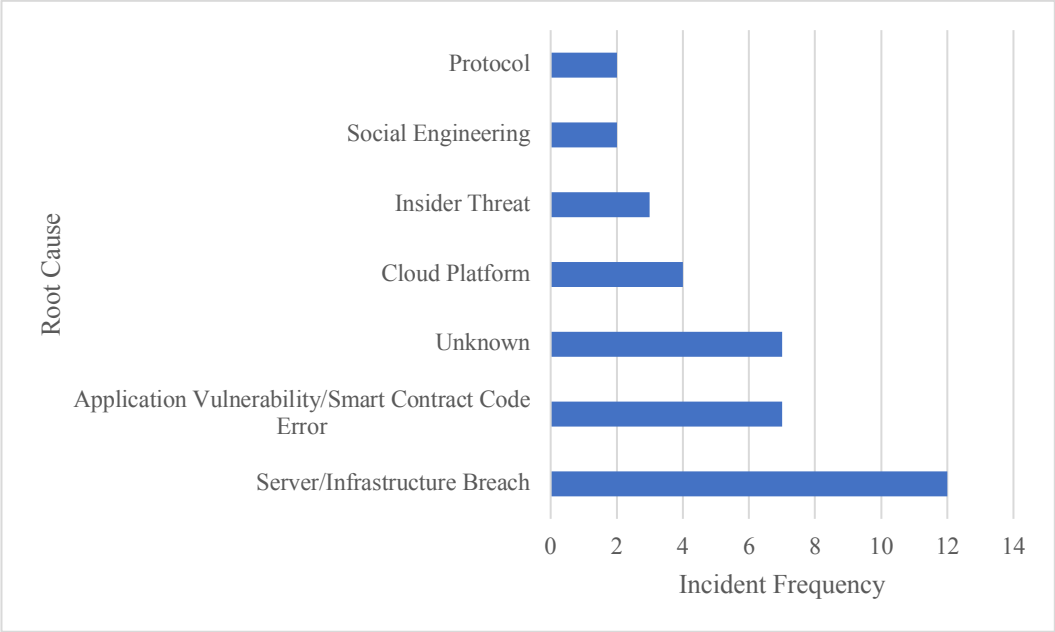

Figure 2. Root Cause Analysis